DETAILED ACTION

The instant application having Application No. 10/588460 is presented for examination by the examiner. Claims 16, 18-21, and 23-31 are pending.

Response to Arguments

Applicant's arguments filed 3/15/11 have been fully considered but they are not persuasive. Applicant alleges that the combination of Watanabe and Yamaguchi do not render the claims obvious. Specifically it is asserted that the combination does not disclose storing the encrypted biometric signature in the device to which the user requests access and transferring the encrypted biometric signature from the device to the electronic chip. Applicant purports this statement because he insists that Yamaguchi does not teach storing the encrypted biometric signature at the computer to which the user requests access. This point is moot because the primary reference, Watanabe, was relied up to teach this feature. As explained in the previous Office Action, Watanabe teaches having the IDC (encrypted biometric signature) at the device to which the user wants to access (Fig. 24). In Fig. 27, the IDC is shown to be stored on the IC when again it is in close proximity to the device to which access is sought. All that is relied upon in Yamaguchi is that a computer can store large quantities of encrypted biometric signatures provides motivation as to why it would have been obvious to one of ordinary skill in the art to try store them on the computer. Both Watanabe and Yamaguchi teach, the IDC can be stored on the device or the IC

(Yamaguchi fig. 42, and 0044). There is no reason to assume the computer to which access is sought could not store the encrypted biometric signatures. Applicant's remarks still seem to overcomplicate the combination of the two references. All the pieces are there in the primary reference and the secondary reference provides the motivation as to why one of ordinary skill in the art would try the specific combination as claimed. It would have been obvious to one of ordinary skill in the art to take advantage of both the large storage space in the computer and the security of the IC card to complete the biometric authentication.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 16, 18-21, and 23-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over USP Application Publication 2002/0069361 to Watanabe et al., hereinafter Watanabe in view of USP Application Publication 2001/0036301 to Yamaguchi et al., hereinafter Yamaguchi.

As per claim 16, Watanabe teaches a method of securing access to a piece of equipment, the method comprising:

obtaining a reference datum for an authorized user, in an authentication medium, wherein said reference datum comprises at least an encrypted authentic biometric signature [IDC] (0356);

storing an encrypted version of said authentic biometric signature on said piece of equipment (0335);

acquiring, at a sensor, a plain biometric signature for a user requesting access to said piece of equipment (0357);

decrypting, in said authentication medium, said encrypted authentic biometric signature (0356);

verifying, in said authentication medium, the authenticity of said plain biometric signature by comparing said plain biometric signature of said user with said decrypted authentic biometric signature of an authorized user (0357); and

granting said user access to said piece of equipment if said comparison is successful and denying access if said comparison fails (0357). While Watanabe teaches many embodiments of securing access to a piece of equipment, he is silent in explicitly disclosing a single embodiment teaching all of the above mentioned limitations combined with storing said encrypted authentic biometric signature on a piece of equipment and transmitted it to the authentication medium. Watanabe does teach storing the encrypted profile on computers in other embodiments. Moreover, Yamaguchi teaches that encrypted biometric templates are stored on a computer (see Figure 42 and paragraphs 0040 and 0044-46). Yamaguchi teaches hundreds of templates can be stored on a traditional computer database and hard drive. It is known that smart cards have limited memory. It is inherent that if the encrypted biometric sample is stored on the computer, and the IC card is performing the comparison, then the encrypted biometric sample must be sent to the IC card. In the cited Watanabe embodiment, the IC card obtains both the encrypted biometric sample and the input biometric sampling for authentication. The claim would have been obvious because combining known methods which produce similar results is within the capabilities of one of ordinary skill in the art. Watanabe teaches the encrypted biometric signature is decrypted in the smart card; the same result is achieved whether it was always stored there, or was retrieved from a computer database.

As per claim 21, Watanabe teaches a method of securing access to a piece of equipment, the method comprising:

creating a reference datum for an authorized user in an authentication medium comprising an electronic chip card, separate from said piece of equipment, wherein the creation of said reference datum (0198) comprises:

(i) inputting a personal identification code for said authorized user
on a keyboard (0198 and 0248);

(ii) detecting, at a sensor, a plain authentic biometric signature for
said authorized user (0198);

(iii) encrypting said plain authentic biometric signature by means of
a private key (0198 and 0199);

(iv) sending said encrypted authentic biometric signature to said piece of equipment (0234);

(v) associating said personal identification code with said encrypted authentic biometric signature (0248); and

(vi) storing said encrypted authentic biometric signature and said associated personal identification code on said computer (0248);

receiving a personal identification code inputted on a keyboard (0248);

acquiring, at a sensor, a plain biometric signature of a user requesting access to said piece of equipment (0357); and

verifying the authenticity of said plain biometric signature for a user requesting access to said piece of equipment, wherein said verifying comprises:

(i) matching said personal identification code with an encrypted authentic biometric signature stored on said computer (0554);

(iii) decrypting said authentic biometric signature, on said authentication medium, by means of a private key on said authentication medium (0357);

(iv) comparing, on said authentication medium, said decrypted authentic biometric signature with said plain biometric signature of said user requesting access to said piece of equipment, to provide a comparison result (0357); and

(v) granting access to said user requesting access to said piece of equipment if said comparison result is successful and denying access if said comparison result fails (0357).

While Watanabe teaches many embodiments of securing access to a piece of equipment, he is silent in explicitly disclosing a single embodiment teaching all of the above mentioned limitations combined with storing said encrypted authentic biometric signature on a piece of equipment and transmitted it to the authentication medium. Watanabe does teach storing the encrypted profile on computers in other embodiments. Moreover, Yamaguchi teaches that encrypted biometric templates are stored on a computer (see Figure 42 and paragraphs 0040 and 0044-46). Yamaguchi teaches hundreds of templates can be stored on a traditional computer database and hard drive. It is known that smart cards have limited memory. It is inherent that if the encrypted biometric sample is stored on the computer, and the IC card is performing the comparison, then the encrypted biometric sample must be sent to the IC card. In the cited Watanabe embodiment, the IC card obtains both the encrypted biometric sample and the input biometric sampling for authentication. The claim would have been obvious because combining known methods which produce similar results is within the capabilities of one of ordinary skill in the art. Watanabe teaches the encrypted biometric signature is decrypted in the smart card; the same result is achieved whether it was always stored there, or was retrieved from a computer database.

As per claims 18 and 23, Watanabe teaches said electronic card includes a decryption module (0356).

As per claims 19 and 24, Watanabe teaches said electronic card includes a comparison module, and said comparing is performed in said electronic card (0357).

As per claims 20 and 25, Watanabe teaches said electronic card further comprises an encryption module (0346 and 0352). Examiner supplies the same rationale as recited in the rejection of claim 16 to store the encrypted biometric signature on the computer.

As per claim 26, Watanabe teaches a device for securing access to a piece of equipment, comprising:

a storage device in said piece of equipment, for storing an encrypted authentic biometric signature (0336) and a corresponding personal identification code of an authorized user (0554);

a sensor for acquiring a plain biometric signature of a user requesting access to said piece of equipment (0357); and

an authentication medium comprising an electronic chip card (IC) having a controller, wherein said controller:

decrypts said authentic biometric signature by means of a secret key (0356);

compares said decrypted authentic biometric signature with said plain biometric signature of said user requesting access to said piece of equipment, to provide a comparison result; and grants access to said user requesting access to said piece of equipment if said comparison is successful and denying access if said comparison fails (0357).

While Watanabe teaching many embodiments of securing access to a piece of equipment, he is silent in explicitly disclosing a single embodiment teaching all of the above mentioned limitations combined with receiving said encrypted authentic biometric signature from said storage device, associated with said personal identification code **in the authentication medium**. Watanabe does teach storing the encrypted profile on computers in other embodiments. Moreover, Yamaguchi teaches that encrypted biometric templates are stored on a computer associated with said piece of equipment (see Figure 42 and paragraphs 0040 and 0044-0046). Yamaguchi teaches hundreds of templates can be stored on a traditional computer database and hard drive. It is known that smart cards have limited memory. It is inherent that if the encrypted biometric sample is stored on the computer, and the IC card is performing the comparison, then the encrypted biometric sample must be sent to the IC card. In the cited Watanabe embodiment, the IC card obtains both the encrypted biometric sample and the input biometric sampling for authentication. The claim would have been obvious because combining known methods which produce similar results is within the capabilities of one of ordinary skill in the art. Watanabe teaches the encrypted biometric signature is decrypted in the smart card; the same result is achieved whether it was always stored there, or was retrieved from a computer database.

As per claim 27, Watanabe teaches at least one computer for storing a plurality of encrypted authentic biometric signatures and a corresponding plurality of personal identification codes for a corresponding plurality of authorized users [inherent this registration process applies to more than one user; 0234], wherein said at least one computer:

Watanabe does not explicitly teaches delivering an encrypted authentic biometric signature to said authentication medium when receiving an access request from a user, such that said authentication medium is capable of providing a plurality of users secure access to said piece of equipment. Examiner supplies the same rationale for combining the feature of storing the signatures in a computer until the access attempt as taught by Yamaguchi and recited in claim 26.

As per claim 28, Watanabe teaches said authentication medium is an electronic card having a memory storing a secret key that cannot be read from outside [smart cards are known for their protected memory].

As per claim 29, Watanabe teaches an encryption module that encrypts an authentic biometric signature supplied in plain form to said sensor and delivers said encrypted authentic biometric signature to said at least one computer, in response to an encryption command (0234). Examiner supplies the same rationale as recited in the rejection of claim 16 to store the encrypted biometric signature on the computer.

As per claim 30, Watanabe teaches said secret key is a private key having a matching public key, and wherein said encryption module is included in said at least one computer and uses said matching public key to encrypt authentic biometric signatures (0235).

As per claim 31, Watanabe teaches said piece of equipment includes an encryption module for encrypting an authentic biometric signature for storage in said piece of equipment (0228).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to MICHAEL R. VAUGHAN whose telephone number is (571)270-7316. The examiner can normally be reached on Monday - Thursday, 7:30am - 5:00pm, EST. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan Flynn can be reached on 571-272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/M. R. V./

Examiner, Art Unit 2431

/NATHAN FLYNN/
Supervisory Patent Examiner, Art Unit 2431